

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-044607

(43)Date of publication of application : 14.02.2003

(51)Int.Cl.

G06F 17/60

(21)Application number : 2001-273520

(71)Applicant : NIPPON TELEGR & TELEPH CORP  
<NTT>

(22)Date of filing : 10.09.2001

(72)Inventor : NISHIDA GEN  
TAKAKURA TAKESHI  
HAYASHI RYOICHI

(30)Priority

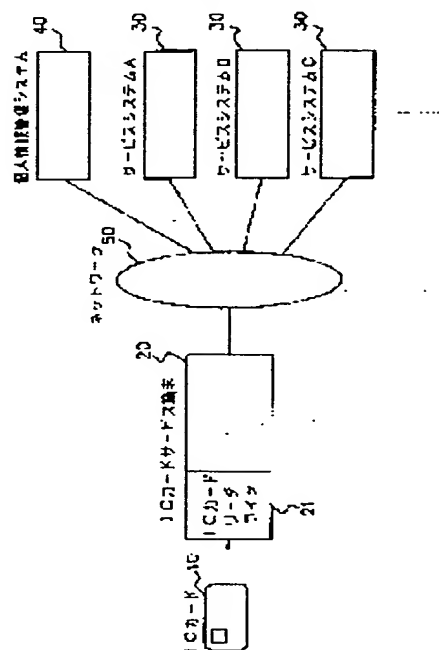
Priority number : 2001152377 Priority date : 22.05.2001 Priority country : JP

## (54) SYSTEM FOR INTEGRATED MANAGEMENT OF PERSONAL INFORMATION

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a system for integrated management of personal information by which a user himself or herself can manage personal information on the user and which allows personal information needed by the system to be used under conditions permitted by the user.

**SOLUTION:** An IC card service terminal 20 having an IC card reader/writer to transmit and receive data to from an IC card 10 stored the personal information, a plurality of service systems 30 providing service to the user via the IC card 10 and the service terminal 20 by using the personal information stored in the IC card 10 and a personal information management system 40 providing service to manage the personal information of the user stored into the IC card 10 are connected via a network 50, so that a personal information management system 40 can provide the personal information to each service system 30 within the ranges permitted by each user.



## LEGAL STATUS

[Date of request for examination] 13.07.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

**BEST AVAILABLE COPY**

[Number of appeal against examiner's decision  
of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-44607

(P2003-44607A)

(43)公開日 平成15年2月14日(2003.2.14)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
G 0 6 F 17/60	1 3 2	G 0 6 F 17/60	1 3 2
	5 1 0		5 1 0
	5 1 2		5 1 2

審査請求 未請求 請求項の数16 O L (全 14 頁)

(21)出願番号 特願2001-273520(P2001-273520)  
(22)出願日 平成13年9月10日(2001.9.10)  
(31)優先権主張番号 特願2001-152377(P2001-152377)  
(32)優先日 平成13年5月22日(2001.5.22)  
(33)優先権主張国 日本(J P)

(71)出願人 000004226  
日本電信電話株式会社  
東京都千代田区大手町二丁目3番1号  
(72)発明者 西田 玄  
東京都千代田区大手町二丁目3番1号 日  
本電信電話株式会社内  
(72)発明者 ▲高▼倉 健  
東京都千代田区大手町二丁目3番1号 日  
本電信電話株式会社内  
(74)代理人 100069381  
弁理士 吉田 精孝

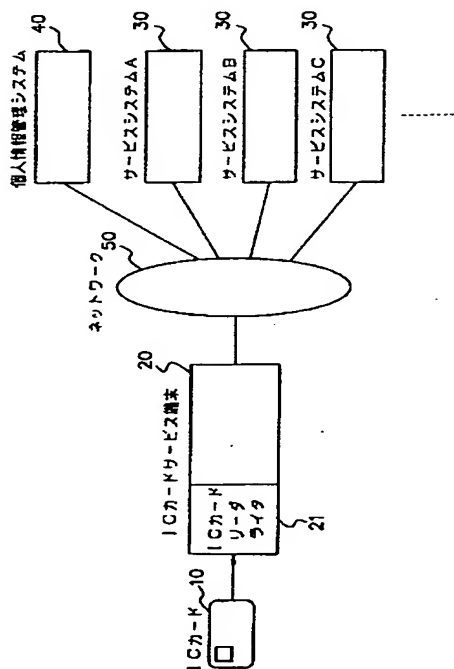
最終頁に続く

(54)【発明の名称】 個人情報統合管理システム及びそのプログラム並びにそのプログラムを記録した媒体

(57)【要約】

【課題】 ユーザの個人情報をユーザ自身が管理でき、サービスシステムが必要とする個人情報はユーザが許可した条件下でのみ利用可能となし得る個人情報統合管理システムを提供すること。

【解決手段】 個人情報を格納したICカード10との間でデータを送受信するためのICカードリーダライタを有するICカードサービス端末20と、ICカードに格納されたユーザの個人情報を利用し、ICカード10及びICカードサービス端末20を通じてユーザにサービスを提供する複数のサービスシステム30と、ICカード10に格納されたユーザの個人情報を管理するサービスを提供する個人情報管理システム40とをネットワーク50を介して接続することにより、個人情報管理システム40から各サービスシステム30へのユーザが許可した範囲での個人情報の提供を可能とする。



【特許請求の範囲】

【請求項1】 少なくともユーザの個人情報を格納したICカードと、ICカードとの間でデータを送受信するためのICカードリーダライタを有するICカードサービス端末と、ICカードにICカード用アプリケーションプログラムを提供するとともにICカードサービス端末に端末用アプリケーションプログラムを提供し、各アプリケーションプログラムが起動したICカード及びICカードサービス端末を通じてユーザにサービスを提供する複数のICカードサービスシステムと、ICカードサービス端末と複数のICカードサービスシステムとを接続するネットワークとからなり、前記ICカードサービスシステムとして、

ICカードに格納されたユーザの個人情報を利用してユーザにサービスを提供するサービスシステムを少なくとも1つ具備し、かつ、

ICカードに格納されたユーザの個人情報を管理するサービスを提供する個人情報管理システムを具備したことを特徴とする個人情報統合管理システム。

【請求項2】 前記ICカードサービスシステムとして、前記に加え、ICカードに本システムにおけるユニークなユーザIDを払い出す機能と、個人情報を初期入力する機能と、入力した情報を参照し、確認し、保存する機能とを有するICカード登録アプリケーションを実行する個人情報登録システムを具備したことを特徴とする請求項1に記載の個人情報統合管理システム。

【請求項3】 前記ユーザの個人情報は、ユーザIDを含む個人を特定する又は特徴づけるための基本情報と、各サービスシステムを利用する際に使用するアプリケーション個人情報と、前記個人情報管理システム及び前記サービスシステムを利用する際に取得した個人履歴情報と、これら基本情報、アプリケーション個人情報及び個人履歴情報の各項目についての利用条件を定めた利用条件情報とからなり、

前記サービスシステムは、該サービスシステムを特定する又は特徴づけるためのサービスシステム情報と、該サービスシステムが独自に収集した該サービスシステムの利用者の顧客情報と、ICカードに格納された個人情報のうちユーザが該サービスシステムに対して定めた利用条件の範囲で複製した個人情報とを格納し、

前記個人情報管理システムは、ICカードに格納された個人情報のうちユーザが該個人情報管理システムに対して定めた利用条件の範囲で複製した個人情報と、サービスシステムに格納されたサービスシステム情報のうちサービスシステムが許可した範囲で複製したサービスシステム情報とを格納することを特徴とする請求項1または2に記載の個人情報統合管理システム。

【請求項4】 前記サービスシステムは、ICカードに格納された個人情報のうちユーザが該サー

ビスシステムに対して定めた利用条件の範囲で複製した個人情報と、該サービスシステムが独自に収集した該サービスシステムの利用者の顧客情報とを格納する顧客情報データベースと、

該サービスシステムが提供するサービスをユーザの要求に応じて処理するサービス処理モジュールとにより構成されることを特徴とする請求項1または2に記載の個人情報統合管理システム。

【請求項5】 前記ICカードサービス端末は、ユーザの要求に基づき該ユーザがサービスシステムを利用した時の個人履歴情報をICカードに送信する機能を有し、前記ICカードは、ICカードサービス端末から送信された個人履歴情報を蓄積する機能を有することを特徴とする請求項1または2に記載の個人情報統合管理システム。

【請求項6】 前記ICカードは、ICカードサービス端末から送信されたサービスシステム毎にフォーマットが異なるサービス利用時の個人履歴情報を、統一されたフォーマットの個人履歴情報に変換する機能を有することを特徴とする請求項5に記載の個人情報統合管理システム。

【請求項7】 前記個人情報管理システムは、ICカードに格納された個人情報のうちユーザが該個人情報管理システムに対して定めた利用条件の範囲で複製した個人情報を格納する個人情報データベースと、サービスシステムに格納されたサービスシステム情報のうちサービスシステムが個人情報管理システムに対して定めた利用条件の範囲で複製したサービスシステム情報を格納するサービスシステムデータベースと、個人情報管理システムにアクセスするユーザの認証と、アクセス対象となった個人情報の利用条件情報の解析と、ユーザの個人情報操作内容を解釈し該操作が意味する個人情報管理サービスの実行とを行う個人情報管理モジュールと、

個人情報管理システムにアクセスするサービスシステムの認証と、アクセス対象個人情報の利用条件情報の解析と、サービスシステムが個人情報管理システムに要求する処理内容の判断とを行うサービスシステム管理モジュールと、

個人情報管理モジュールやサービスシステム管理モジュールにおける、個人情報データベースやサービスシステムデータベースから読み出した情報を処理し、個人情報管理システム外部に出力する際に該情報に対する利用条件を設定し、該利用条件情報に基づき利用制御する利用制御モジュールとにより構成されることを特徴とする請求項1または2に記載の個人情報統合管理システム。

【請求項8】 前記個人情報管理システムは、前記サービスシステムの要求に基づき、該サービスシステムの顧客情報と、該個人情報管理システムの個人情報とを結び付け、

結び付けた連携情報は、該個人情報の利用条件情報と、該サービスシステムのサービスシステム情報から個人情報管理システムが許可した内容とによる利用制御に基づいた提供がなされる情報連携機能を有することを特徴とする請求項1乃至7のいずれかに記載の個人情報統合管理システム。

【請求項9】 顧客情報と個人情報との関連付けを行う前記情報連携機能は、サービスシステムに対し匿名性を維持して処理することを特徴とする請求項8に記載の個人情報統合管理システム。

【請求項10】 前記情報連携機能は、ICカードに格納された個人情報を、ユーザIDを含む形で個人情報管理システムの個人情報データベースに格納する第一の事前処理ステップと、ICカードまたは個人情報管理システムにおいて暗号鍵と復号鍵と鍵IDとを作成し、暗号鍵と鍵IDをICカードに格納し、復号鍵と鍵IDを個人情報管理システムの復号鍵データベースに格納する第二の事前処理ステップと、

ICカードにおいてユーザIDを第二の事前処理ステップで得た暗号鍵で暗号化した暗号化ユーザIDを生成して格納する第三の事前処理ステップと、

ICカードからサービスシステムに暗号化ユーザIDと鍵IDを送信するサービス利用ステップと、サービスシステムから個人情報管理システムに顧客情報と暗号化ユーザIDと鍵IDとを送信する第一の連携処理ステップと、

個人情報管理システムにおいて鍵IDを用いて復号鍵データベースから該鍵IDに対応する復号鍵を検索し、該復号鍵で暗号化ユーザIDを復号してユーザIDを特定する第二の連携処理ステップと、

個人情報管理システムにおいてユーザIDを用いて個人情報データベースから該ユーザIDに対応する個人情報を検索し、顧客情報と検索から得られた個人情報とを連携付ける第三の連携処理ステップとを含む処理によって実現されることを特徴とする請求項8または9に記載の個人情報統合管理システム。

【請求項11】 少なくともユーザの個人情報を格納したICカードと、ICカードとの間でデータを送受信するためのICカードリーダーライタを有するICカードサービス端末と、ICカードにICカード用アプリケーションプログラムを提供するとともにICカードサービス端末に端末用アプリケーションプログラムを提供し、各アプリケーションプログラムが起動したICカード及びICカードサービス端末を通じてユーザにサービスを提供する複数のICカードサービスシステムと、ICカードサービス端末と複数のICカードサービスシステムとを接続するネットワークとからなり、前記ICカードサービスシステムとして、

ICカードに格納されたユーザの個人情報を利用してユ

ーザにサービスを提供するサービスシステムを少なくとも1つ具備し、

かつ、

ICカードに格納されたユーザの個人情報を管理するサービスを提供する個人情報管理システムを具備した個人情報統合管理システムのプログラムであって、該プログラムはコンピュータ上に、

ICカードに格納された個人情報のうちユーザが該サービスシステムに対して定めた利用条件の範囲で複製した個人情報と、該サービスシステムが独自に収集した該サービスシステムの利用者の顧客情報とを格納する顧客情報データベースと、

該サービスシステムが提供するサービスをユーザの要求に応じて処理するサービス処理モジュールとにより構成されるサービスシステムを実現することを特徴とする個人情報統合管理システムのプログラム。

【請求項12】 少なくともユーザの個人情報を格納したICカードと、ICカードとの間でデータを送受信するためのICカードリーダーライタを有するICカードサービス端末と、ICカードにICカード用アプリケーションプログラムを提供するとともにICカードサービス端末に端末用アプリケーションプログラムを提供し、各アプリケーションプログラムが起動したICカード及びICカードサービス端末を通じてユーザにサービスを提供する複数のICカードサービスシステムと、ICカードサービス端末と複数のICカードサービスシステムとを接続するネットワークとからなり、前記ICカードサービスシステムとして、

ICカードに格納されたユーザの個人情報を利用してユーザにサービスを提供するサービスシステムを少なくとも1つ具備し、

かつ、

ICカードに格納されたユーザの個人情報を管理するサービスを提供する個人情報管理システムを具備した個人情報統合管理システムのプログラムであって、該プログラムはコンピュータ上に、

ICカードに格納された個人情報のうちユーザが該個人情報管理システムに対して定めた利用条件の範囲で複製した個人情報を格納する個人情報データベースと、サービスシステムに格納されたサービスシステム情報のうちサービスシステムが個人情報管理システムに対して定めた利用条件の範囲で複製したサービスシステム情報を格納するサービスシステムデータベースと、

個人情報管理システムにアクセスするユーザの認証と、アクセス対象となった個人情報の利用条件情報の解析と、ユーザの個人情報操作内容を解釈し該操作が意味する個人情報管理サービスの実行とを行う個人情報管理モジュールと、

個人情報管理システムにアクセスするサービスシステムの認証と、アクセス対象個人情報の利用条件情報の解析

と、サービスシステムが個人情報管理システムに要求する処理内容の判断とを行うサービスシステム管理モジュールと、

個人情報管理モジュールやサービスシステム管理モジュールにおける、個人情報データベースやサービスシステムデータベースから読み出した情報を処理し、個人情報管理システム外部に出力する際に該情報に対する利用条件を設定し、該利用条件情報に基づき利用制御する利用制御モジュールとにより構成される個人情報管理システムを実現することを特徴とする個人情報統合管理システムのプログラム。

【請求項13】 前記個人情報管理システムは、前記サービスシステムの要求に基づき、該サービスシステムの顧客情報と、該個人情報管理システムの個人情報とを結び付け、

結び付けた連携情報は、該個人情報の利用条件情報と、該サービスシステムのサービスシステム情報から個人情報管理システムが許可した内容とによる利用制御に基づいた提供がなされる情報連携機能を有することを特徴とする請求項12に記載の個人情報統合管理システムのプログラム。

【請求項14】 顧客情報と個人情報との関連付けを行う前記情報連携機能は、サービスシステムに対し匿名性を維持して処理することを特徴とする請求項13に記載の個人情報統合管理システムのプログラム。

【請求項15】 前記情報連携機能は、ICカードに格納された個人情報を、ユーザIDを含む形で個人情報管理システムの個人情報データベースに格納する第一の事前処理ステップと、

ICカードまたは個人情報管理システムにおいて暗号鍵と復号鍵と鍵IDとを作成し、暗号鍵と鍵IDをICカードに格納し、復号鍵と鍵IDを個人情報管理システムの復号鍵データベースに格納する第二の事前処理ステップと、

ICカードにおいてユーザIDを第二の事前処理ステップで得た暗号鍵で暗号化した暗号化ユーザIDを生成して格納する第三の事前処理ステップと、

ICカードからサービスシステムに暗号化ユーザIDと鍵IDを送信するサービス利用ステップと、サービスシステムから個人情報管理システムに顧客情報と暗号化ユーザIDと鍵IDとを送信する第一の連携処理ステップと、

個人情報管理システムにおいて鍵IDを用いて復号鍵データベースから該鍵IDに対応する復号鍵を検索し、該復号鍵で暗号化ユーザIDを復号してユーザIDを特定する第二の連携処理ステップと、

個人情報管理システムにおいてユーザIDを用いて個人情報データベースから該ユーザIDに対応する個人情報を検索し、顧客情報と検索から得られた個人情報とを連携付ける第三の連携処理ステップとを含む処理によって

実現されることを特徴とする請求項13または14に記載の個人情報統合管理システムのプログラム。

【請求項16】 請求項11乃至15のいずれかに記載のプログラムを記録したことを特徴とするコンピュータ読み取り可能な媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、複数のICカードサービスシステムで使用されるユーザの個人情報を、ユーザ自身が主体的に管理し、かつICカードサービスシステムに必要な個人情報の使用をユーザが設定した利用条件に基づいて制御する、個人情報統合管理システムを実現するための技術に関する。

【0002】

【従来の技術】従来、サービスの提供者が、サービス利用履歴や趣味・嗜好等のユーザの個人情報を管理し、これをユーザに対するマーケティングに活用するケースが数多く見受けられていた。

【0003】近年は、ICカードを用いたICカードサービスシステムを構築して、ユーザ情報の管理を行うシステムが増加している。これは、耐タンパ性に優れたICカードの安全性を活用しようというもので、課金・決済・資産管理サービスのような金銭の出納に関わるサービスや、電子行政・医療情報システムなど、繊細な情報やプライバシーに関わる情報を扱うサービスに対し、暗号・認証技術を用いた堅牢なユーザ認証を実現するために導入されたものである。

【0004】ICカードは、従来の磁気カードと比べ高コストであることから、複数のICカードサービスシステムを1枚のカードで共用できるような高機性能性が求められていたが、最近のICチップの演算能力と記憶容量の向上に伴い、1枚のICカードに複数のアプリケーション処理プログラムを搭載することができるようになった。これに併せ、ICカードに搭載するアプリケーションについても、共通の開発環境と実行環境を提供するプラットフォームが開発されている（例えば、NTT技術ジャーナル、2000年10月号、p.15-18、p.56-59参照）。

【0005】ICカードサービスシステム開発の現状を見ると、ICカード媒体の特徴である携行性と安全性を活かしたシステム構築がなされてはいるものの、ICチップの演算処理能力を応用した高機性能性の十分な活用には至っていないようである。

【0006】具体的には、これまでのICカードサービスシステムでは、ICカードからICカードサービスシステムにデータベース処理言語であるSQLコマンドを送信することで、ICカードサービスシステムの個人情報データベースに対する処理を実行する等、ICカードに単なる情報蓄積媒体以上の機能を発揮させていた。

【0007】しかし、ICカード上での処理は、ICカ

ードに蓄積されていた該ICカードサービスシステム向けに用意された処理プログラムとパラメータが選択され起動されるというものであり、高機能ICカードサービスシステムの使い道としては比較的容易な処理内容に過ぎなかった。

【0008】一方、ICカードサービスシステムで使用される個人情報については、上述したように、従来からマーケティングに役立つ情報として認められていたが、近年の通信ネットワークの普及に伴う電子サービスの中で、電子化された個人情報を用いることで容易に実現されるようになったマス・カスタマイゼーションが、マーケティング戦略面のみならず、効率面でも有効であることが判明すると、特に電子化された個人情報の価値はますます増大してきた。事実、通信ネットワーク上でのサービス提供企業が売却される際に、該企業の有する個人情報重要な資産価値として認められもしている。

【0009】しかしながら、個人情報が電子化され通信ネットワーク上で利用されることには、ユーザとして安全面での懸念がある。セキュリティ、プライバシーの問題がそれである。個人情報保護に関する法律制定の動きもあるが、ユーザも自己防衛を考えるようになり、また、サービス提供者としても信用問題につながるため、相当の力を入れるようになってきつつある。

【0010】通信ネットワークにおける個人情報流通を技術面から支えるため、暗号・認証やデータ利用制御技術が開発され、後者においては、ユーザがユーザ自身の個人情報に利用条件を課す方法が考案されている（例えば、寺西裕一 他「利用規約に基づくマルチメディアコンテンツ流通システムの設計」情報研報99-DPS-95、Vol. 99、No. 94、1999、pp31-36参照）。これは、個人情報の管理に対しユーザが主導権を持つことにつながり、また、個人情報が通信ネットワーク上を流通する世界を想定したものである。

【0011】

【発明が解決しようとする課題】このような状況の下、多数のICカードサービスシステム導入の動きがあるが、現状のままでICカードサービスシステムの構築が進められると、ユーザの個人情報が複数のICカードサービスシステムで独立に存在し、各ICカードサービスシステムで管理されることになる。すると、ユーザの個人情報は各ICカードサービスシステムで管理され、ICカードサービスシステムの数だけ存在することになるので、ユーザは利用したいシステムの数だけICカードを携帯する必要が生じ、ユーザ自身の個人情報であるにも拘わらず、ユーザ自身で管理することができず、ユーザの個人情報に何らかの変更が生じた場合、複数のシステムに対してそれぞれ個人情報更新処理を行わなければならない。また、ユーザはユーザ自身の個人情報がどこでどのように使用されているか把握できず、個人情報がユーザの意図に沿わない使われ方をされる可能性が

ある。

【0012】そこで、本発明では、ICカードサービスシステム毎に管理されているユーザの個人情報を、ユーザ自身が管理できるようにし、各ICカードサービスシステムが必要とする個人情報をユーザが許可した条件の下でのみ利用可能とし、ICカードサービスシステムに提供した個人情報の使われ方を制御できる個人情報統合管理システムを提供することを目的とする。

【0013】また、派生的課題として、ICカードサービスシステム間で個人情報を流通する際に、ユーザが予想していないシステム間の情報連携により、個人のプライバシーに関わる情報が生じる危険がある。そこで、このような個人情報を生成しない、または、生成されても利用を制御可能にする技術を提供することも、本発明で解決すべき課題である。

【0014】

【課題を解決するための手段】上記の課題を解決するために、本発明では、ICカードの多機能性を従来以上に発揮させ、1枚のICカードに複数のサービス処理機能を持たせてワンカード化を図り、また、暗号・認証技術と利用制御技術を利用して、個人情報の安全な流通の仕組みを設ける。そして、ICカードと複数のICカードサービスシステムが相互に情報連携しての処理が可能となるICカードサービス環境を構築する。

【0015】具体的には、ICカード上に、個人情報と該個人情報の利用条件情報とを蓄積し、更に、複数のICカードサービスシステムのICカードにおける処理プログラム（カード用サービスAP）及びこれに用いる情報（AP個人情報）を、複数サービス分だけ搭載する。この時、ICカードサービスシステムの1つとして、ユーザの個人情報を管理するサービスを行う個人情報管理システムを用意し、該システムのICカードにおける処理プログラム（カード用管理AP）をICカードに搭載しておく。

【0016】ICカードサービス端末は、ユーザからの要求に基づいて、ユーザがサービスシステムを利用した時に該サービスシステムが収集した情報をICカードに送信し、ICカードのカード用管理APは受信したサービス利用に関する情報を、そのサービスシステム毎に異なるフォーマットを適当なフォーマットに揃えて個人履歴情報として蓄積する。

【0017】個人情報管理システムは、複数のユーザの個人情報及び各個人情報に課した利用条件情報及び通常の各ICカードサービスシステム（以下、サービスシステムと略す）のAP個人情報を各ユーザが主体となって管理する機能と、各ユーザの個人情報を各ユーザの利用条件情報に基づいて制御する機能を、個人情報管理システムのサービスとして提供する。また、個人情報管理システムは、サービスシステム情報を管理する機能を有する。そして、あるサービスシステムに対する個人情報を

用いた処理においては、該サービスシステムに対応するサービスシステム情報と個人AP情報を参照することで、個人情報の利用制御や、情報連携サービスや、カード用サービスAPの処理制御を行う。

【0018】一方、システム間での情報連携が個人のプライバシーを侵害するのを防ぐために、サービスシステムの顧客情報と、管理システムの個人情報を匿名のまま関連付ける仕組みを設ける。

【0019】ユーザ個人を識別するためのユーザIDを暗号化した暗号化ユーザIDと、暗号鍵を識別する鍵IDを設定し、サービスシステムに提供する個人情報に暗号化ユーザIDと鍵IDを付加する。

【0020】また、管理システムでは、鍵IDに対応した復号鍵を検索できるように復号鍵を格納する復号鍵データベースを構築する。

【0021】

【作用】本発明の個人情報統合管理システムは、個人情報管理サービスを提供する個人情報管理システムと、各種サービスを提供する複数のサービスシステムと、カードリーダーライタが付属したICカードサービス端末と、そして、各ユーザの個人情報等を蓄積したICカードにより構成される。ICカード上には、個人情報管理システムで管理する個人情報と該個人情報の利用条件情報とを蓄積し、更に、複数のサービスシステムのカード用サービスAP及びAP個人情報を搭載する。ここで、ICカード上の個人情報の個人履歴情報は、サービス利用時にサービスシステムからICカードサービス端末を通じて送信されるものである。

【0022】個人情報統合管理システムでは、ICカードサービスシステムの1つとして個人情報管理システムを用意し、ユーザの個人情報を管理するサービスを行う。個人情報管理サービスを利用するには、ICカードサービス端末で、カード用個人情報管理AP(カード用管理AP)をICカードに予めダウンロードする。そして、ユーザはICカードサービス端末(カード端末)で個人情報管理サービスのクライアントプログラム(端末用管理AP)を起動する。

【0023】個人情報管理システムは、複数のユーザの個人情報及び各個人情報に課した利用条件情報及び各サービスシステムの個人AP情報を各ユーザが主体となって管理する機能と、各ユーザの個人情報を各ユーザの利用条件情報に基づいて制御する機能を、個人情報管理システムのサービス(管理サービス)として提供する。

【0024】ユーザが各サービスシステムのサービスを利用するには、カード端末で、利用する各サービスシステムのカード用サービスAPを予めICカードにダウンロードする。そして、ユーザはICカードサービス端末(カード端末)で利用したいサービスシステムのクライアントプログラム(端末用サービスAP)を起動する。端末用サービスAPは、カード用管理APが管理する個

人情報及び利用条件情報と、カード用サービスAPが管理する個人AP情報を利用して、各サービスシステムが提供する様々な処理を行う。

【0025】個人情報管理システムの管理サービスは、サービスシステムの個人情報要求に対し、ユーザが設定した個人情報と利用条件情報とを用い、ユーザが許可した範囲で個人情報を提供する。ICカードがシステムに接続されていない場合も、管理サービスは利用条件付き個人情報を提供できる。

【0026】個人情報管理システムとサービスシステムとの情報連携については、サービスシステムから個人情報管理システムに情報連携処理要求があると、管理システムは適切な復号鍵を検索し、暗号化ユーザIDを復号してユーザIDを特定し、該ユーザIDの個人情報と関連付ける。この関連付け処理では、ユーザIDをシステム処理の工程内でのみ使用しているので、結果を抽出する前に利用条件に基づく利用制御を行うことで、プライバシーを侵害するような情報連携を避けることができる。

【0027】

【発明の実施の形態】本発明の個人情報統合管理システムの実施の形態の一構成例について、図1を用いて説明する。

【0028】図1において、10はICカード、20はICカードサービス端末(以下、カード端末と略す)、30は複数の通常のICカードサービスシステム(以下、サービスシステムと略す)、40は個人情報管理システム、50はネットワークである。

【0029】本発明の個人情報統合管理システムでは、カード端末20と、複数のサービスシステム30と、個人情報管理システム40とがネットワーク50を介して接続されている。これらに加え、各ユーザのICカード10が、単体では機能しないが、カード端末20のICカードリーダーライタ(ICカードRW)21に挿入されることでシステムの一部として動作する。

【0030】更に、システムには、ユーザが初めてICカードサービス環境である個人情報統合管理システムにアクセスしようとする際に、該ユーザに初期情報を記録したICカードを発行する個人情報登録システムが接続されていても良い。本発明ではこの個人情報登録システムを必須の構成要素とはしないが、個人情報統合管理システムの中で絶対の信頼機関として個人情報登録システムを使用する構成も可能である。

【0031】これら個人情報統合管理システムを構成する各構成要素が格納・管理している情報を図2に示す。項目に記した具体的なプロパティは、情報のカテゴリを分かり易く示すための例である。尚、図2において、ハッチングが施してある部分は情報が原本であることを意味している。ここでいう原本とは、各構成要素が主体となって管理する、つまり優先的に扱う情報という意味で

考えて良い。また、ICカードは記憶容量に制限があるので、カード用管理アプリケーションプログラム(A P)で蓄積するデータはポイントとして機能する情報であっても良い。

【0032】ICカード10にはユーザの個人情報が格納されている。個人情報には、ユーザを特定する又はユーザを特徴づけるための住所、氏名、年齢、性別、趣味、嗜好……といった情報等の基本情報と、各サービスシステムのアプリケーションを利用する際に必要なAP個人情報と、個人情報管理システム及び各サービスシステムを介して利用してきたログ情報である個人履歴情報と、そして、これら基本情報・AP個人情報・個人履歴情報の個々の項目についての利用条件を定めた利用条件情報とがある。

【0033】サービスシステム30には、サービスシステム情報と、顧客情報と、AP個人情報とが格納されている。サービスシステム情報は、該サービスシステムが主体となって管理する、サービスシステムを特定・識別する又はサービスシステムの特徴を示す情報である。顧客情報は、該サービスシステムが主体となって管理する、サービスシステム利用ユーザ毎に取得した情報である。AP個人情報は、ICカード10に格納しているAP個人情報の中で、ユーザがサービスシステムに利用を許可している情報であり、ユーザ数の分だけ存在する。

【0034】個人情報管理システム40では、ユーザが主体となって管理している、ICカードに格納する個人情報の全て又は個人情報に課せられた利用条件情報が個人情報管理システムに許す範囲の個人情報を格納している。加えて、サービスシステムが主体となって管理しているサービスシステム情報を、各サービスシステムの分だけ管理している。

【0035】個人情報統合管理システムを利用しようとするユーザは、ユーザ自身の個人情報を管理するために、個人情報管理システム40の個人情報管理サービス(管理サービス)を使用する。ICカード情報を可視化し、情報を操作するソフトウェアがあれば管理はできるが、ICカード情報をオンラインで扱うためには、個人情報管理システムが必要になる。

【0036】個人情報管理サービスの概要を図3及び図4を用いて説明する。

【0037】図3は個人情報管理システムの概要を示すもので、図中、41は個人情報データベース、42はサービスシステムデータベース、43は個人情報管理モジュール、44はサービスシステム管理モジュール、45は利用制御モジュールである。また、図4は個人情報管理サービスの処理の流れを示す。

【0038】初めて個人情報管理システム40にアクセスするユーザは、予めカード端末20でICカード10にカード用個人情報管理AP(以下、カード用管理APと略す)11をダウンロードする。そして、管理サービ

スを利用する場合、ユーザはカード端末20で端末用個人情報管理AP(以下、端末用管理APと略す)22を起動し、カード端末20のICカードRW21に挿入したICカード10上のカード用管理AP11を用いて、個人情報及び各個人情報に対する利用条件の設定など、個人情報管理の操作を行う。

【0039】ユーザは、管理サービスを利用して設定した個人情報及び利用条件情報の原本を、ICカード10上のカード用管理AP11に保存する。個人情報管理システム40の個人情報管理モジュール43では、カード用管理AP11の個人情報と利用条件情報を、管理システム40に対し定めた利用条件の範囲で個人情報管理システム40の個人情報DB41に保存する。個人情報管理システム40に対して定める個人情報の利用条件としては、個人情報の全てを取り扱うことができるように特権システムとして定めることが望ましいが、必要ならば適当な利用条件を定めることで利用制御させることも可能である。

【0040】尚、個人情報管理システム40中、サービスシステムDB42、サービスシステム管理モジュール44及び利用制御モジュール45については、図7、8を用いて後ほど説明することとし、管理サービスの処理の流れを説明する。

【0041】カード端末20で端末用管理AP22を起動しておき、そこにICカード10が挿入されるとICカード10上のカード用管理AP11が起動され、管理サービスが可能になる。カード用管理AP11は、本管理サービスのサービス認証を行い、該サービスに対する利用条件を判断の上、開示制御を加えた個人情報の読み出しを行う。

【0042】一方、個人情報管理システム40の個人情報管理モジュール43は、ICカード利用者のユーザ認証を行い、システム上の個人情報DB41から利用条件を判断しながら個人情報の読み出しを行う。これらの個人情報は端末用管理AP22に送信され、具体的なユーザの管理操作を受け付ける管理サービスが提供される。

【0043】ユーザがカード端末20で個人情報操作の管理サービス処理を行うと、処理内容に応じ、ICカード10または個人情報管理システム40に処理内容が送信、処理される。処理が終わればカード端末20に処理完了の通知が返り、ICカード10上のカード用管理AP11が終了し、カード端末20での操作に従い、ICカード10が排出される。

【0044】次に、サービスシステムによる提供サービスの概要を図5及び図6を用いて説明する。

【0045】図5はサービスシステムの概要を示すもので、図中、31はサービスシステム顧客データベース、32はサービス処理モジュールである。また、図6はサービスシステムにおける提供サービスの処理の流れを示す。

【0046】初めてサービスシステム30にアクセスするユーザは、カード用管理AP11に加え、カード用サービスAP12をICカード10に搭載しておく必要があり、予めカード端末20で該サービスのカード用サービスAP12をICカード10にダウンロードしておく。

【0047】サービスシステム30のサービスを受けるには、カード端末20で端末用サービスAP23を起動する。この時、既にICカード10に搭載されているカード用管理AP11で保存している個人情報、サービスに対し定められた利用条件情報の下で利用可能になる。端末用サービスAP23は、必要に応じてICカード10上のカード用サービスAP12及びカード用管理AP11と連携して、必要な個人情報を該サービスに課せられた利用条件情報に基づき利用しつつ、該サービスのサービス処理を遂行する。

【0048】サービスシステム30では、サービス処理モジュール32を介し、カード用管理AP11によって利用制御された個人情報を用いてサービス処理が行われ、サービスシステム30が自身で収集したユーザ情報を顧客情報として収集する。

【0049】サービスシステム30の処理の流れとしては、まず、カード端末20で端末用サービスAP23を起動しておき、そこにICカード10を挿入する。サービスシステム30では、ICカード利用者のユーザ認証を行い、サービスシステム30に格納されているサービスシステム情報を読み出す。ICカード10では、カード用サービスAP12の前にカード用管理AP11が起動される。カード用管理AP11はサービスシステム情報を参照し、利用しようとしているサービスシステム30の認証を行う。そして、該サービスに対する利用条件を判断の上、開示制御を加えた個人情報の読み出しを行う。

【0050】ICカード10上で動作するAPの制約から、APの複数起動が可能な場合と不可能な場合とがある。図6の例では、カード用管理AP11とカード用サービスAP12の双方のAPが同時に起動しないと仮定して、カード用管理AP11を終了させた後、カード用サービスAP12を起動している。

【0051】カード用サービスAP12の起動を受けて、端末用サービスAP11はICカード10からサービスに用いる情報の読み出しを行い、また、サービスシステム30からは顧客DB31から顧客情報の読み出しを行う。これらの情報は端末用サービスAP23に送信され、具体的なユーザの操作を受け付けるサービス提供が開始される。ユーザがカード端末20でサービス操作を行うと、処理内容に応じ、ICカード10またはサービスシステム30に処理内容が送信、処理される。

【0052】ICカード10とサービスシステム30での各々の処理の結果、必要に応じてICカード10また

は顧客DB31に処理情報の書き込みが行われる。例えば、売買に関するサービスが行われた場合を考えると、売買情報はサービスシステム30の顧客DBに書き込まれるだけでなく、ユーザの要求に基づき、カード端末20を介してICカード10にも送信される。ICカード10では、サービスシステム毎にフォーマットが異なる前記情報を、カード用管理AP11が適当な統一フォーマットの個人履歴情報に変換して該ICカード10内に格納する。

【0053】サービスに関する一連の処理が終わればカード端末20に処理完了の通知が返り、ICカード10上のカード用サービスAP12が終了し、カード端末20での操作に従い、ICカード10が排出される。

【0054】次に、個人情報管理システムの個人情報DBとサービスシステムの顧客情報DBとを連携させるサービスについて図7及び図8を用いて説明する。図7は個人情報管理システム及びサービスシステムの概要を示す。また、図8は連携サービスの処理の流れを示す。

【0055】サービスシステム30は、ICカード10との接続を必要としない処理が目的で個人情報を扱おうとする場合や、統計処理などユーザ一般に関する情報を用いた処理を行う場合等に、個人情報管理システム40の管理サービスを利用する。サービスシステム30の顧客情報と個人情報管理システム40の個人情報を連携させるには、各データベースにユーザを特定するためのキーを設定しておく。この方法の詳細は図9を用いて別途説明する。

【0056】さて、個人情報管理システム40の個人情報管理サービスを利用するサービスシステム30は、個人情報管理システム40のサービスシステム管理モジュール44を介し、サービスシステムDB42にサービスシステム情報を登録しておく必要がある。サービスシステム情報の具体的な項目としては、サービスシステム毎に振られたサービスシステムID、サービスシステムの正当性を認証するための情報、サービスシステムの提供するサービスのカテゴリや特徴的キーワード等が挙げられる。

【0057】個人情報管理システム40は、サービスシステム30の要求に対しサービスシステム管理モジュール44でサービスシステムとしての認証等の処理を行い、利用制御モジュール45で該サービスシステム30の利用条件を判断し、許された範囲内で個人情報DB41から個人情報を抽出し、該個人情報をサービスシステム30に送信する。あるいは定められた利用条件によっては、逆に個人情報管理システム40で該情報を用いた処理を行い、許可された結果のみをサービスシステム30に送信する。

【0058】個人情報管理システムとサービスシステムとの情報連携処理の流れとしては、まず、サービスシステム30から個人情報管理システム40へ、管理サービ

ス利用のためのアクセス要求が送信される。管理システム40はアクセス要求したサービスシステム30の認証を行い、サービスシステムDB42からサービスシステム情報の読み出しを行う。

【0059】サービスシステム30は、更に、サービスシステム30で得られている顧客情報と個人情報に基づき、管理サービスの個人情報利用要求を送信する。すると管理システム40は、サービスシステム30の顧客IDに対応するユーザIDの個人情報との関連付けを行う。関連付けの方法は、先にも述べたように後述する。管理システム40は、関連付けられた個人情報を個人情報DB41から読み出し、該個人情報の利用条件を解析し、利用条件付き個人情報を生成する。サービスシステム30は、自ら所有する顧客情報に利用条件を設定して、これを管理システム40に送付する。

【0060】この時点で個人情報管理システム40にユーザに関する各種情報が取り揃えられたことになるが、個人情報管理システム40では、利用制御モジュール45において、個人情報と顧客情報を連携させ、連携情報に対しどのような利用条件情報を付与すれば良いかの解析を行う。そして、その判断に基づき、利用条件付きの連携情報が生成され、管理サービスの処理結果としてサービスシステム30に利用条件付き連携情報を引き渡す。

【0061】以上が一連の処理の流れであるが、利用条件に依っては、最後の工程で連携情報がサービスシステム30に引き渡されず、個人情報管理システム40上でのみ取り扱い可能な状態になることもある。このような時、もしもサービスシステム30に連携情報入手の許可は無くても、連携情報を使った別の処理が許可されていれば、個人情報管理システム40の利用制御モジュール45において処理が行われ、サービスシステム30に処理結果を返送することになる。

【0062】次に、ICカード10から個人情報管理システム40に送信され格納されている個人情報とサービスシステム30に格納されている顧客情報との連携サービスの実現例を図9を用いて説明する。ここでは、不必要な個人情報の公開を防ぐため、匿名性を維持しつつ顧客情報に対応する連携先個人情報を判断する方法を例示する。

【0063】個人情報管理システム40には、ICカード10の個人情報が、ユーザが設定した利用条件と共に格納されている(ステップ1-1)。これに加え、ICカード10または個人情報管理システム40で暗号鍵と復号鍵のペアを作成し、鍵IDを付与しておく。そして、ICカード10に暗号鍵と鍵IDを格納し、また、個人情報管理システム40の復号鍵DB46に復号鍵と鍵IDを格納しておく(ステップ1-2)。

【0064】ICカード10では、ユーザIDを暗号鍵で暗号化した暗号化ユーザID(暗号化UID)を生成

する(ステップ1-3)。ユーザがサービスシステム30のサービスを受ける際には、該暗号化UIDと鍵IDをサービスシステム30に送信し(ステップ2-1)、サービスシステム30は顧客情報を入手する(ステップ2-2)。

【0065】サービスシステム30は、ユーザがサービスを利用する際にユーザから取得した顧客情報を、個人情報管理システム40の個人情報と連携させるために、まず、サービスシステム30から個人情報管理システム40に暗号化UIDと鍵IDとを送信する(ステップ3-1)。

【0066】個人情報管理システム40では、鍵IDを基に復号鍵DBを検索し、鍵IDに該当する復号鍵で暗号化UIDを復号し、ユーザIDを特定する(ステップ3-2)。得られたユーザIDを基に個人情報DB41を検索し、顧客情報と連携させるべき個人情報を得る(ステップ3-3)。

【0067】個人情報管理システム40の利用制御モジュール45は、サービスシステム30に許可された利用条件を判断し、サービスシステム30に提供を許された情報については利用制御を課したまま、個人情報管理システム40からサービスシステム30に送信する。サービスシステム30への該個人情報の提供は許されていないが、顧客情報と個人情報とを用いて行う何らかの処理の結果を知ることが許可されている場合、サービスシステム30から個人情報管理システム40へ該顧客情報を送信し、個人情報と連携させて実行した処理結果をサービスシステム30に返送する。

【0068】サービスシステム30が、個人情報の提供も個人情報を用いた処理の実行も許されていない場合、サービスシステム30から個人情報管理システム40への情報連携要求は不成功に終わる。

【0069】情報連携を用いた具体的な実施サービス例として、また、本発明の個人情報統合管理システムの発展的サービス例として、サービスシステムが顧客情報と個人情報との連携情報を統計情報として顧客動向調査に利用し、抽出した個人に対し広告を配送するサービスについて述べる。

【0070】あるサービスシステム(例えば、SS-Aとする)の顧客情報DBにサービス履歴情報を蓄積しておく。仮に、SS-Aが、SS-Aの提供するサービス甲を受けた顧客に特徴的な傾向を発見したとする。SS-Aは個人情報管理システム40と連携して、前記の特徴的な傾向を見せた顧客の顧客IDと、情報から関連付けられたユーザの個人情報を統計的に提供してもらう。

【0071】この時のユーザの利用条件では、例えば「母数100以上の統計処理への利用を許可」等の設定がなされている必要があり、そのような提供を許可していないユーザの個人情報は、統計情報としても提供されない。SS-Aは、情報連携で得られた統計情報の分析

の結果、例えば「サービス甲を受け、引き続きサービス乙を利用する顧客は20代女性に多数見られる」等のマーケティング情報を得ることができる。

【0072】上記マーケティング情報を得たSS-Aは、サービス甲の利用ユーザの中でまだサービス乙を利用していない顧客に何らかの働きかけを行う、または広く一般ユーザに対して働きかけを行うと考えられる。その働きかけの手段として広告配送による方法がある。しかし、広告配送先である住所情報は、個人情報の1項目であり、SS-Aに公開されるとは限らない。そこで、信用できる機関が広告配送サービスを行う仲介することが考えられる。

【0073】図9における説明では、個人情報管理システムを信用できる機関として、個人情報管理システムで情報連携を行う例を記した。しかし、広告配送専用のサービスシステムB（例えば、SS-B）が信用できるか、またはSS-Bが利用条件を課せられた上でサービスを提供するならば、情報連携をSS-Bで行う方法も採ることができる。実現には、暗号・認証技術と、カプセル化等を用いた利用制御技術を用いた方法が考えられる。

【0074】SS-Bが該サービスを提供する場合、SS-Aは広告情報をカプセル化し、広告情報の内容だけでなくSS-Aが発信者であることも掌握できないような利用条件と共にSS-Bに送り、SS-Bは対応するユーザの個人情報から住所（電子メール広告の場合はメールアドレス）を調べ、関連付けることだけが可能な利用条件を課せられているが、該ユーザのもとに広告情報を配送することは実現できる。

【0075】

【発明の効果】以上述べたように、本発明では、複数のサービスシステムが構築されると、ユーザの個人情報が複数のサービスシステムで独立に存在し、各サービスシステムで管理されることになるところを、個人情報を各サービスシステムで統一的に管理するための個人情報管理システムを設けることで、個人情報の一元的な管理を共通のサービス環境で実現している。

【0076】これにより、ユーザは1枚のICカードで複数のサービスシステムを利用できるようになり、また、ユーザがその個人情報をユーザ自身で管理することが可能になり、また、ユーザの個人情報を1度更新するだけで各サービスシステムに行き届かせることができる。そして、ユーザ自身の個人情報にユーザ自身が利用

条件を課することで、個人情報管理システムに保存した個人情報がどのように利用されているかを情報収集することが可能になる。

【0077】サービス提供者にとっては、本発明により、従来収集していた顧客の個人情報がサービスシステムの顧客情報DBに格納できなくなるという弊害がある。しかし、顧客情報管理に要する余分な設備投資や運用稼働を必要としないため、コストを抑えることができる。また、個人情報管理主体がユーザに戻ったことで、個人情報の信頼度が高まり、サービスシステム側で個人情報管理責任を負わなくて良いという効果がある。

【0078】更に、顧客情報と個人情報を連携する仕組みをユーザの個人情報の匿名性に留意しつつ実現することで、従来の機能、即ちユーザが要望としている広告情報等のサービスに関する情報を入手する機能と、サービスシステムが要望している個人情報をを用いたマーケティング情報を入手する機能とを維持することができる。

【図面の簡単な説明】

【図1】本発明の個人情報統合管理システムの実施の形態の一例を示す構成図

【図2】本システムの各構成要素に格納される個人情報の具体例を示す説明図

【図3】個人情報管理システムの概要を示す構成図

【図4】個人情報管理サービスの処理の流れ図

【図5】サービスシステムの概要を示す構成図

【図6】サービスシステムにおける提供サービスの処理の流れ図

【図7】個人情報管理システム及びサービスシステムの概要を示す構成図

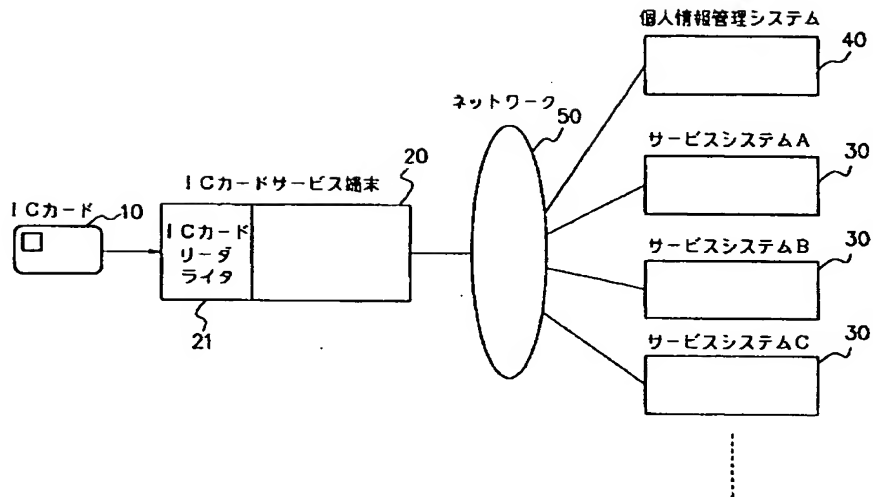
【図8】個人情報管理システムとサービスシステムとの連携サービスの処理の流れ図

【図9】連携サービスの実現例を示す説明図

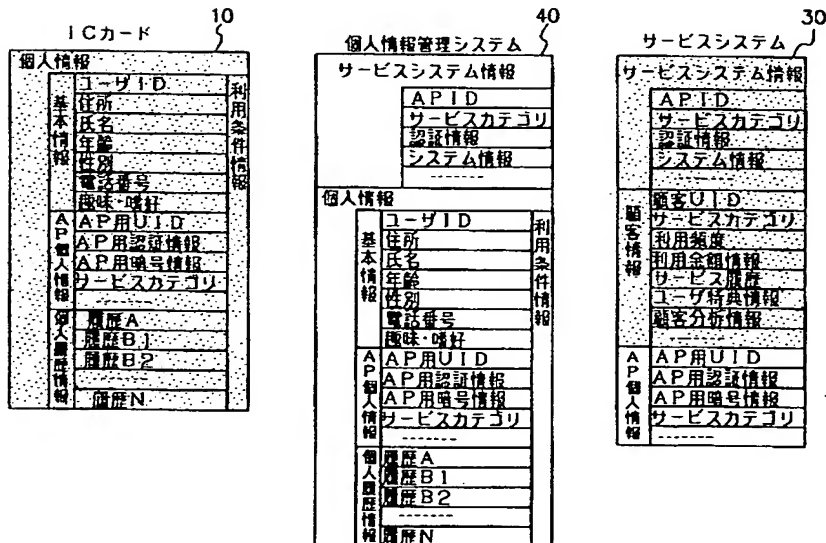
【符号の説明】

10：ICカード、11：カード用管理AP、12：カード用サービスAP、20：ICカードサービス端末、21：ICカードRW、22：端末用管理AP、23：端末用サービスAP、30：サービスシステム、31：サービスシステム顧客DB、32：サービス処理モジュール、40：個人情報管理システム、41：個人情報DB、42：サービスシステムDB、43：個人情報管理モジュール、44：サービスシステム管理モジュール、45：利用制御モジュール、50：ネットワーク。

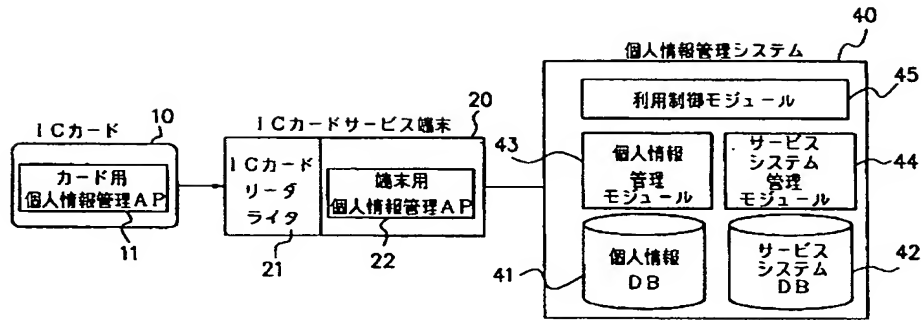
【図1】



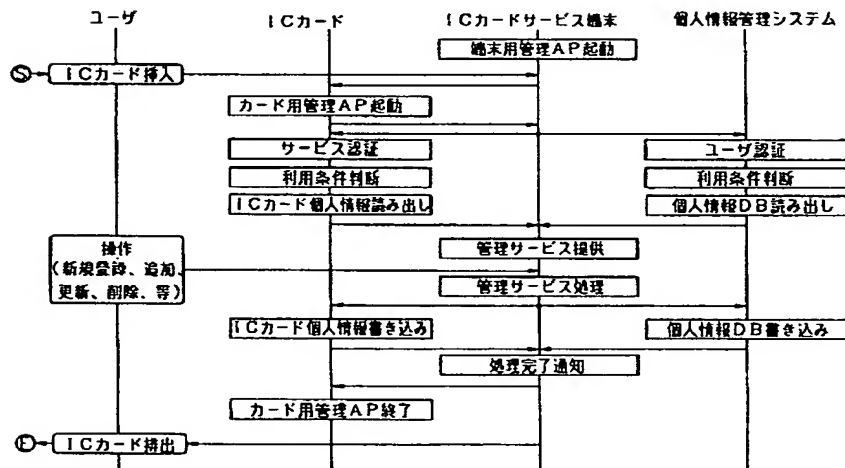
【図2】



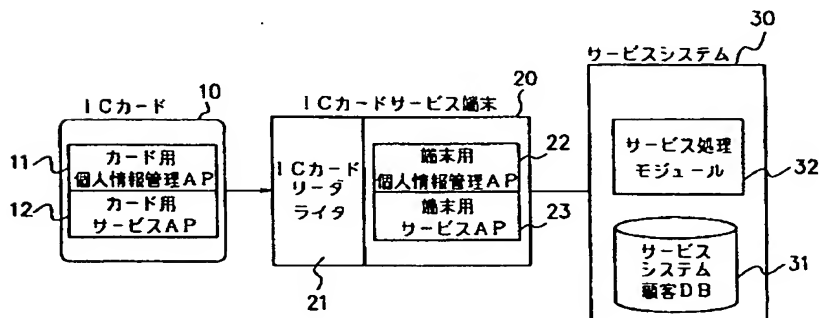
【図3】



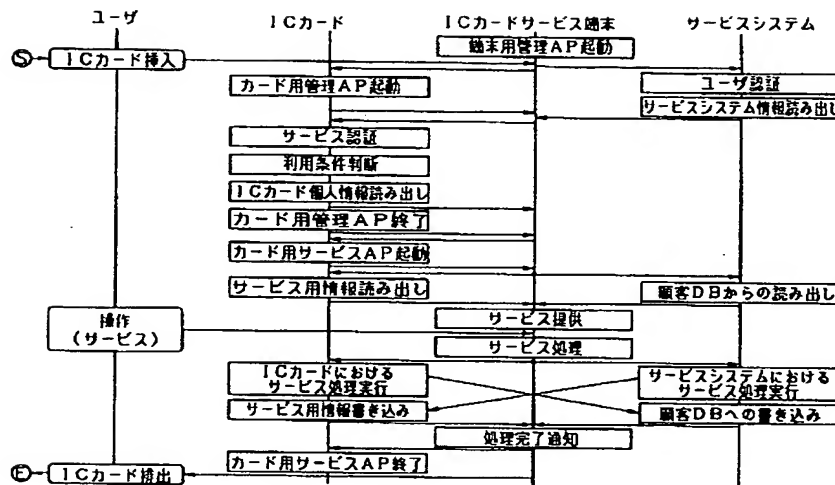
【図4】



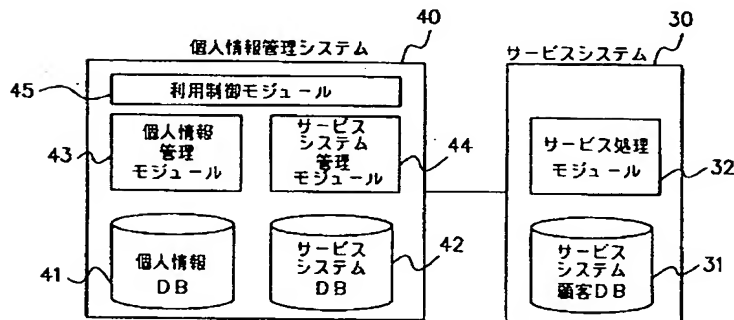
【図5】



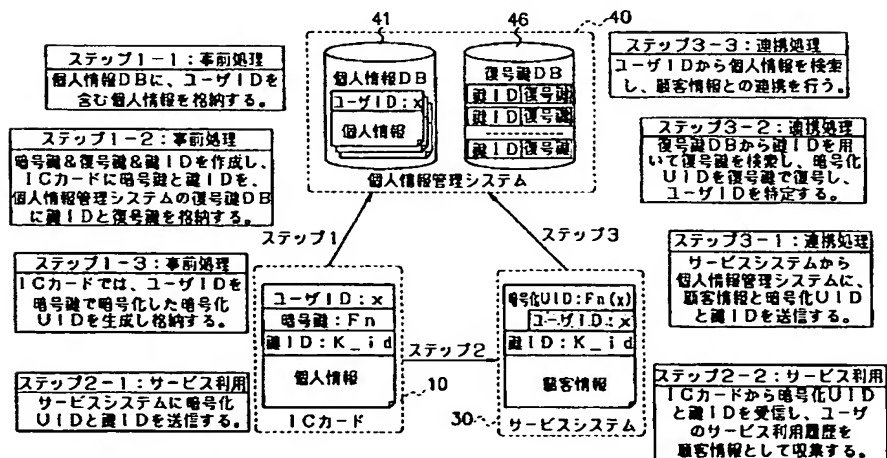
【図6】



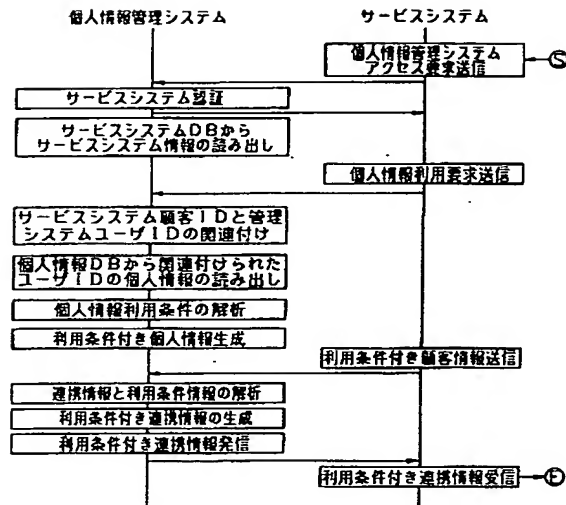
【図7】



【図9】



【図8】



フロントページの続き

(72)発明者 林 良一  
東京都千代田区大手町二丁目3番1号 日  
本電信電話株式会社内

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ BLACK BORDERS

☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

☒ FADED TEXT OR DRAWING

☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING

☐ SKEWED/SLANTED IMAGES

☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS

☐ GRAY SCALE DOCUMENTS

☒ LINES OR MARKS ON ORIGINAL DOCUMENT

☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**